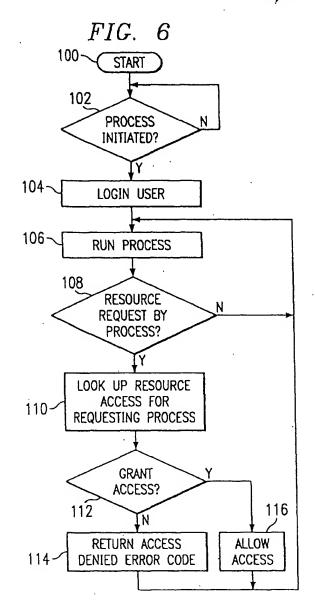
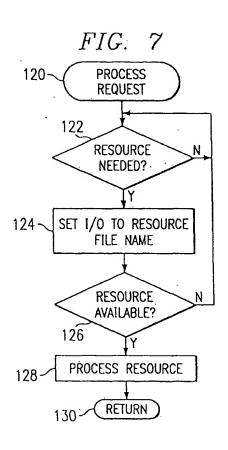
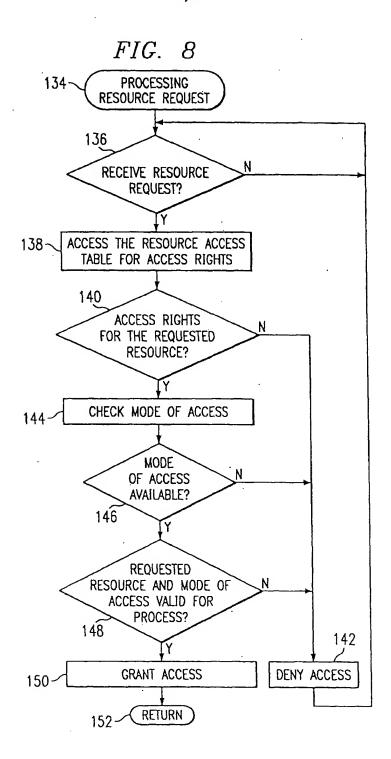


4/7

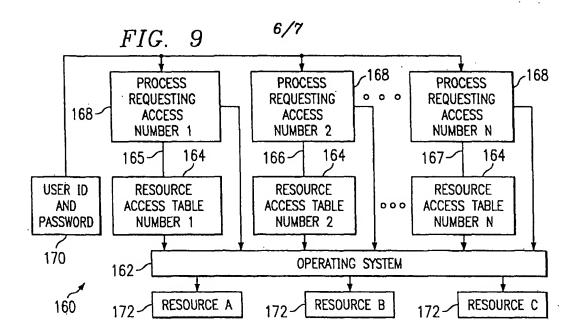


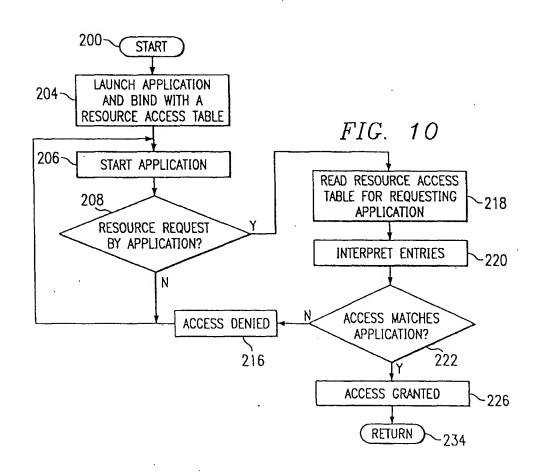


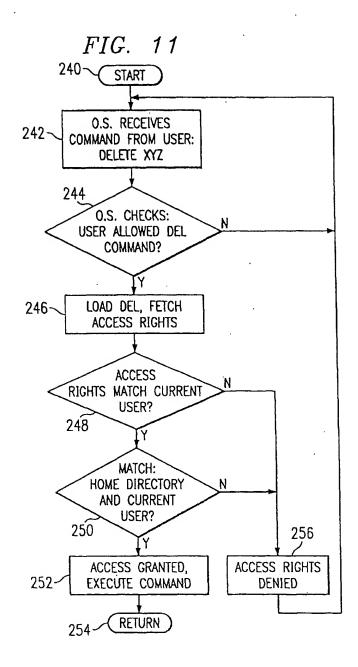
5/7

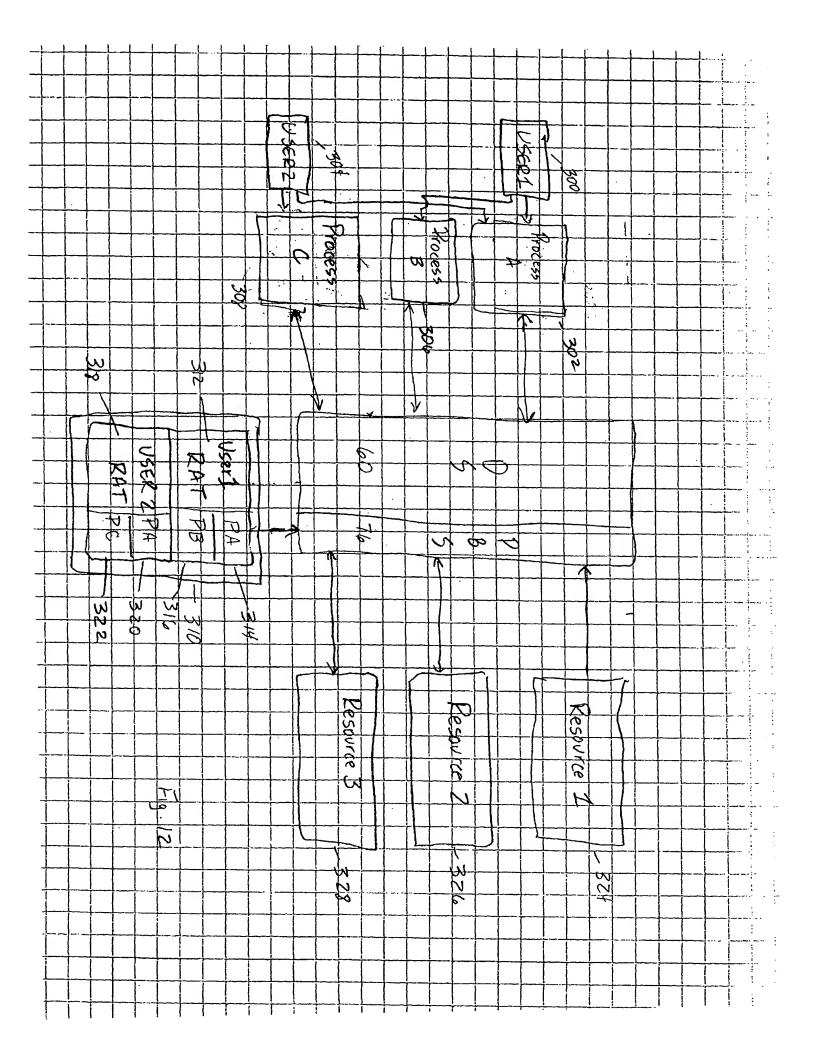


.)









- i -		Figure 1	3			-		 	+	-	1 : ·
: !	11:1-		-		<u> </u>	-		- 			
·	User/Chent	Process						<u>catio</u>	<u> </u>	_ - -	<u></u>
! 		Authenti			- - -	Mc	dule		+		
	 	CLOGI	N.EX	€)		+ + +		 	+		
+			=		1						
 	Initiate				332						ļ
330	Authentication			Randem	322				+	- 	
 		Ner	nber	(RN)	1	> _G	renero	te R	2	334	·
 			-			+					
344	Enter Username,		-			, M	lodify	Proce	2551	330	
	Password							truct			
-											T
:						\$	tore '	RN	! !-	338	
,								1 !			
						K	send	RN	1	340	
344	Generate Hosh								11	1	
	(Password + RN)										
					1	! ! !		 	11		
	Send Username,		-		1	1 1 1	— -	} 	1-1		
346	Hash		-		1		_		+++		
	17050		7			1 1			+		210
			+		+++	-		k Pro	; ,	- 4	1 2
			+	 				ture fo		ding	
					+++	+	HUth	nticat	ادما		-
++					+++	+			1 -		
+				 			Ketri	eve F	§N		350
: 					+++			 -	-		<u></u>
							Ketrie	ve B	skwor	9	352
				-	- -	+ + +	<u>associ</u>	ated v	4#	JSern	ame
+									1		<u></u> :
- +	+						Gener	ate H	xsh	_	354
 						+ + +	(Passu	prd +	3N)		
						+ + +					
<u> </u>					$\perp \perp \perp$		Compo	re Ho	sh V	alkes	356
	++++								$\perp \perp$	-	
 							Maduf	y Proc	e55'	Task	353
· !							Struc	ture			
- 											
;		Set us	er =	302			Confi	m Aut	hent	coto	
		Usern	ì	-			set v	ser =	user	nam	e 360
. :					7 11				7	 -	

			Figure 14					
			J ;					
	:	· · · · · · · · · · · · · · · · · · ·		· · ·				
- ; ;		Set Password		 	Authent	ication	· · · · · · · · · · · · · · · · · · ·	
: ·						+++		
	36	4			+			
		Enter Username			+			
	368				- 		+ :-	
		Enter Old Rossword.			10.11	tication	366	
			+++	\\\\				
					Proces	55		
			-!-!-!	- 	Cac	a Quthent	vention.	369
	*				- CONTIN	TANK INCHI	: :	
	370	Enter New	-					
		Possword			-			1
				_ +				
1						Passwar		372
					in as	sociation	with	
!					userr	20 me		
								<u> </u>
					1		_	
					+			
							- 	
								
					+		,	
								
	_				+			<u> </u>
								
					+++	+++		+
								+
			+++		+ + +			
					++++	++++		
- - 					+ + +	+ + + + + +		
				!				

	1		Fig. 15	
		- 		
		Key Exchan	ge	
	Client	++++	Server	
	74 Request Key Excl	na nae		+++++++++++++++++++++++++++++++++++++++
	275 Send Usernan			
	Enter Password		Modify Task Structu	re 376
	511		3	
			Generate RN1	373
			Send RN1	380
				
382			Retrieve Password (F	
PAR	Calculate hash		associated with user	name
	+ + + + + + + + + + + + + + + + + + + +		calculate hash	384
			H(PW, RN1)	789
386	Key = H(PWF	(INS	Key 1 = H (PW, RN:	1) 398
			Generate RN2	390
	++++++		Send RNZ	392
			calculate hash	20.
304	salculate hash		H(PW, RNZ)	396
	H(PW, RNZ)		THE PARTY OF A	
			Key 2 = H(PW RNZ	398
400	Key Z= H(PW)	RN2)		
	++++++		Modify Task Structure	402
				++
		-		
				+++++
				
				+ + +

